REMARKS

Claims 1-36 are pending in the present application as amended. Independent claims 1, 9, 19, and 27 have been amended. No claims have been canceled or added. Support for the amendments to the claims may be found at least at, for example, paragraph 0022 et seq. of the application as filed. Accordingly, Applicants respectfully submit that no new matter has been added to application by the Amendment.

The Examiner has rejected claims 1-5, 9-15, 19-23, and 27-33 under 35 U.S.C. § 102(e) as being anticipated by Rothrock (U.S. Pat. No. 7,174,320). Applicants respectfully traverse the Section 102 rejection insofar as it may be applied to the claims as amended.

As set forth in the specification of the present application, the present invention is generally directed toward the situation where some entity on a computer requires a resource from a software or hardware entity that has been designated the resource provider (RP), and because of the sensitive nature of the resource the RP needs to be able to establish trust in the entity, which has been designated the resource recipient (RR). For example, the RP can be a server or some other source of sensitive data, such as for example a data vault with a sensitive document, and the RR can be a rendering entity that renders an output based on the data, such as a word processor that is to edit or print the sensitive document.

Accordingly, the RP should only provide the resource to the RR if the RR can be authenticated. In the present invention, it is presumed that the RR includes sensitive security information in what has been designated an 'id', and a value designated as a 'code-ID' may be calculated from the RR and the id thereof, perhaps as a hash, where the RP will only provide the resource to the RR if, among other things, an expected code-ID is calculated for the RR. Thus, if the RR or the id thereof are modified, the code-ID calculated therefrom will differ from that which the RP expects, and the RP will refuse to provide a requested resource based on such a differing code-ID.

In particular, in the present invention as recited in independent claim 1, an RR operating on a computing device requests a resource from an RP that is a software or hardware construct, and the RR has an id that includes security-related information specifying an environment in which the RR operates. The RR and the id are loaded onto the computing device and a corresponding code-ID is calculated based on the RR and id. The

RR requests the resource from the RP, and it is ascertained that the requesting RR has rights to the resource and is to be trusted with the resource.

In addition, the request for the resource is forwarded from the RR to the RP, and includes the calculated code-ID for the requesting RR, the id for the requesting RR, and a definition of the resource requested by the RR. Thus, the RP verifies that the calculated code-ID in the forwarded request matches one of one or more valid code-IDs for the identified RR, concludes based thereon that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon which the RR operates is known security-related information that can be presumed to be trustworthy, and responds to the forwarded request by providing the requested resource. Upon receiving same, the RR employs the resource in a manner consistent with the trust imparted to the RR by the RP, and in accordance with the security-related information set forth in the id corresponding to the RR.

Independent claim 9 recites subject matter similar to that of claim 1, but from the point of view of the RP. In particular, in claim 9, the RP verifies the received request, obtains the code-ID, the id, and the definition of the resource requested from the received request, identifies the RR and obtains each of one or more valid code-IDs for the identified RR, and verifies that the calculated code-ID in the received request matches one of one or more valid code-IDs for the identified RR. With such verification, the RP can then conclude that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon which the RR operates is known security-related information that can be presumed to be trustworthy.

Independent claims 19 and 27 recites subject matter similar to that of claims 1 and 9, respectively, although in the form of a computer-readable medium with computer-executable instructions for performing the respective methods.

The Rothrock reference discloses providing adaptive security for access to content, where a content license associated with the content is examined to determine if a user has rights to such access. Specifically, a security factor value is calculated and then compared to a corresponding value set within the license. Notably, the Rothrock license is for a piece of Rothrock content, and is therefore not akin to an id that describes sensitive security information for a resource requester (RR), as is required by claims 1, 9, 19, and 27. That is,

the id for an RR is not a content license corresponding to content but instead describes security information for an RR that is to receive content.

In the main, the Examiner refers to the flow charts set forth in Figs. 6 and 7 of the Rothrock reference as 'inherently' disclosing the invention recited in the claims rejected under Section 102. However, and significantly, such flow charts disclose a method whereby an agent verifies signatures and identities, performs re-hashing to update an image map in a secure storage, and also performs continuous integrity verification based on security factors in the secure storage. Notably, such a Rothrock agent is not a resource provider (RP), as is recited in claims 1, 9, 19, and 27, especially inasmuch as such agent does not provide any content or other resource.

At any rate, the Rothrock reference does not disclose or even suggest the specific steps performed to impart trust to a RR as are recited in the independent claims of the present application. Specifically, the Rothrock reference does not disclose or suggest calculating a code-ID for an RR based on the RR and an id that has security environment information for the RR, and forwarding the calculated code-ID to the RP, as is particularly required by claims 1 and 19. Likewise, the Rothrock reference does not disclose or suggest that the RP verifies that the calculated code-ID in the forwarded request matches one of one or more valid code-IDs for the identified RR, concludes based thereon that the RR can be trusted as being a known RR that can be presumed to be trustworthy, and also that the security-related information upon which the RR operates is known security-related information that can be presumed to be trustworthy, as is particularly required by claims 9 and 27.

Moreover, Applicants respectfully note that the rejection of the claims by the Examiner relies in large part on the argument that "Rothrock *inherently* discloses the method of securely obtaining a content access as described in the instant claims." Office Action at 3, emphasis added. Applicants respectfully disagree, and also respectfully submit that such a broad statement of disclosure is inappropriate and does not satisfy the requirement that the Examiner particularly point out how each element and limitation of the claims is present in the cited Rothrock reference, such as is necessary to maintain an anticipation rejection under Section 102.

Applicants respectfully point out that, according to MPEP section 2112, the fact that a certain result or characteristic, such as a series of method steps being performed, may occur

or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. In re Rijckaert, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); In re Oelrich, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is *necessarily* [emphasis added] present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " In re Robertson, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

To summarize, then, inherency is established only if an element, or series of elements in the present context, are *necessarily* present in Rothrock reference, and not merely by the possibility that such elements could be present. That said, Applicants respectfully submit that the argument for inherency as set forth by the Examiner does not even remotely rise to the level of a possibility that the method steps of claims 1, 9, 19, and 27 are present in the Rothrock reference, let alone that such elements are necessarily present. Instead, Applicants respectfully submit that there is not even a hint that the Rothrock agent or any other entity in the Rothrock reference performs the particular method steps of claims 1, 19, 19, and 27. The Rothrock system does not inherently calculate a code-ID such as that recited in the claims, which is based on an RR and an if for the RR, and does not inherently employ such a code-ID in the manner recited in such claims. That is, the Rothrock reference not only makes no reference to such a code-ID, but also makes no reference to any process or structure that necessarily requires such a code-ID. Thus, no such code-ID or method steps employed to generate and employ such a code-ID can be inherently found in the Rothrock reference as being necessary to the operation of the Rothrock system.

Accordingly, for all of the aforementioned reasons, Applicants respectfully submit that the Rothrock reference does not anticipate claims 1, 9, 19, or 27, or any claims depending therefrom, including claims 2-5, 10-15, 20-23, and 28-33. As a result, Applicants respectfully request reconsideration and withdrawal of the Section 102 rejection.

The Examiner has also rejected claims 6-8, 16-18, 24-26, and 34-36 under 35 U.S.C. § 103(a) as being obvious over the Rothrock reference in view of Mourad et al.(U.S. Pat. No. 7,171,558). Applicants respectfully traverse the Section 103 rejection insofar as it may be applied to the claims as amended.

Applicants respectfully note that inasmuch as independent claims 1, 9, 19, and 27 have been shown to be unanticipated and are non-obvious, then so too must all claims depending therefrom be unanticipated and non-obvious, including such claims 6-8, 16-18, 24-26, and 34-36, at least by their dependencies. As a result, Applicants respectfully request reconsideration and withdrawal of the Section 103 rejection.

In view of the foregoing Amendment and Remarks, Applicants respectfully submit that the present application including claims 1-36 is in condition for allowance and such action is respectfully requested.

Respectfully submitted,

Date: September 4, 2007

/Joseph R. Condo/
Joseph R. Condo
Registration No. 42,431

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439